Power of Anisotropic Exchange Interactions: Universality and Efficient Codes for Quantum Computing

L.-A. Wu and D. A. Lidar
Chemical Physics Theory Group, University of Toronto, 80 St. George St., Toronto, Ontario M5S 3H6, Canada

We study the quantum computational power of a generic class of anisotropic solid state Hamiltonians. A universal set of encoded logic operations are found which do away with difficult-to-implement single-qubit gates in a number of quantum computer proposals, e.g., quantum dots and donor atom spins with anisotropic exchange coupling, quantum Hall systems, and electrons floating on helium.We show how to make the corresponding Hamiltonians universal by encoding one qubit into two physical qubits, and by controlling nearest neighbor interactions.

While decoherence is the most significant fundamental obstacle in the path towards the construction of a quantum computer (QC), in the realm of scalable QC proposals [1–7] a pressing concern is the technological difficulty of implementing single-qubit operations together with two-qubit operations. In general these two types of operations may impose very different constraints, or single-qubit operations may be hard. E.g., in the proposals utilizing quantum dots [1], donor-atom nuclear [2] or electron [3] spins, and quantum Hall systems [4], single-qubit operations require control over a local magnetic field, are significantly slower than two-qubit operations (mediated by an exchange interaction), and require substantially greater materials and device complexity. In the quantum dots in cavities proposal [5] each dot needs to be illuminated with a separate laser, and reduction in the number of lasers by elimination of single-qubit operations is a potentially significant technical simplification. In the electrons-on-helium proposal [7] single-qubit operations require slow microwave pulses, limiting the number of logic operations executable before decoherence sets in. It is thus clear that quite generally a significant gain may be had by enabling quantum logic operations to be performed through two-qubit operations only. The need for single-qubit operations arises from the "standard paradigm" of (non fault-tolerant) universal quantum computation, which prescribes the use of single-qubit Hamiltonians that can generate all one-qubit quantum gates [$SU(2)$] together with a two-body interaction that can generate an entangling two-qubit gate such as CNOT [8]. The universality of this set essentially amounts to its ability to generate $SU(2^N)$ with N qubits [9]. While it was recognized early on that a universal QC can be constructed using at most two-body interactions [10], the abstract theory hardly makes reference to the "natural talents" of a given quantum system as dictated by its intrinsic Hamiltonian. Indeed, most discussions of universality, e.g., [11], rather than using the physical notion of Hamiltonians, are cast in the computer-science language of unitary gates (exponentiated Hamiltonians). Based on these observations a new paradigm was recently proposed in [12], termed "encoded-universality" (EU): to study the quantum computational power of a system *as embodied in its naturally available Hamiltonian*, by using encoding [encoded gates – consisting of sequences of physical gates – act on encoded (logical) qubits generating $SU(2^M)$, where M is the dimension of the code space]. Earlier work [13–16] had implicitly studied EU constructions. In this work we introduce a general formalism, discovered by a mapping of qubits to parafermions that will be described elsewhere [17], that allows us to quickly assess the quantum computational power of a given Hamiltonian, and construct encoded qubits and operations. Our main result is the classification of the EU power of generic classes of solid-state Hamiltonians, addressing in particular the case of *anisotropic* qubit-qubit interactions pertinent to the quantum Hall [4], quantum dots [5] and atoms [6] in cavities, and the electrons-on-helium [7] proposals. The proposals relying on purely isotropic (Heisenberg) exchange may also benefit from our analysis, in the case that some symmetry breaking mechanism (e.g., surface and interface effects, and/or spin-orbit coupling [18]) introduces anisotropy. For all these cases we give explicit EU constructions which avoid the use of the undesirable single-qubit gates. In particular, we show how to make the anisotropic exchange Hamiltonian universal by *encoding one qubit into two physical qubits*, in contrast to previous results for the Heisenberg case where three physical qubits were required [12,15,16]. Only nearest-neighbor couplings are needed in this construction. Thus we suggest new ways to simplify the operation of a variety of QC proposals, circumventing operations that appear to be dictated by the "standard paradigm".

General analysis. — To set the stage for our discussion of the universality properties of Hamiltonians, let us consider the general structure of operators in the Hilbert space of N qubits in terms of the lowering and raising operators $\sigma_i^{\pm} = (\sigma_i^x \mp i\sigma_i^y)/2$, where $i = 1, ..., N$ and σ_i^α acts non-trivially only on the i^{th} qubit. Define an occupation number $n_i = (1 - \sigma_i^z)/2 = 0$ or 1, which is the number of 1's (up-spins) in the i^{th} position of the vectors of the computational basis, i.e., all length-N bitstrings. The most general operator consistent with $\sigma_i^-\sigma_i^- = \sigma_i^+\sigma_i^+ = 0$ is a linear combination of

$$Q_{\{\alpha\}\{\beta\}} = (\sigma_N^+)^{\alpha_N} \cdots (\sigma_1^+)^{\alpha_1} (\sigma_N^-)^{\beta_N} \cdots (\sigma_N^-)^{\beta_1} \qquad (1)$$

where α_i, β_j can be 0 or 1. There are $2^N \times 2^N$ such operators which form a complete set of generators of the group $U(2^N)$ needed for universal quantum computing [19]. They can be rearranged into certain subsets of operators with clear physical meaning, which we now detail. First, there is a subalgebra with conserved total occupation number, "SAn". This is formed by all operators commuting with the total number operator $\widehat{n} = \sum_i n_i$. Let k (l) be the number of σ_i^+ (σ_i^-) factors in $Q_{\{\alpha\}\{\beta\}}$. SAn consists of the operators for which $k = l$, so the dimension of SAn is $\sum_{n=0}^N \binom{N}{n}^2 = \frac{(2N)!}{N!N!}$. Second, there is a subalgebra with conserved parity, "SAp", i.e., the operators commuting with the parity operator, defined as $\widehat{p} = (-1)^{\widehat{n}}$, with eigenvalues 1 ($-1$) for even (odd) total occupation number. SAp consists of those operators having $k - l$ even, so its dimension is $2^{2N}/2$. Clearly, SA$n \subset$ SAp. Third, there are types of $su(2)$ subalgebras generated by the set $\{Q_{\{\alpha\}\{\beta\}}, Q^\dagger_{\{\alpha\}\{\beta\}}, [Q_{\{\alpha\}\{\beta\}}, Q^\dagger_{\{\alpha\}\{\beta\}}]\}$ in the subspace satisfying the condition $\{Q_{\{\alpha\}\{\beta\}}, Q^\dagger_{\{\alpha\}\{\beta\}}\} = 1$, for specific choices of $\{\alpha\}\{\beta\}$. This results directly in encoding schemes. The following two types of bilinear operators for $i \neq j$: $\sigma_i^+\sigma_j^-$ (which conserve the occupation number), and $\sigma_i^-\sigma_j^-, \sigma_i^+\sigma_j^+$ (which conserve parity), are important examples that illustrate this case. Let $\mu = (ij)$, then

$$T^x_\mu = \sigma_j^+\sigma_i^- + \sigma_i^+\sigma_j^- \text{ and } T^z_\mu = \sigma_i^z - \sigma_j^z \quad (2)$$

generate an $su(2)$ subalgebra, denoted $su^t_\mu(2) \in$SAn.

$$R^x_\mu = \sigma_i^-\sigma_j^- + \sigma_i^+\sigma_j^+ \text{ and } R^z_\mu = \sigma_i^z + \sigma_j^z \quad (3)$$

generate another $su(2)$ subalgebra, denoted $su^r_\mu(2) \in$SAp. It is easy to show that $[su^t_\mu(2), su^r_\mu(2)] = 0$. It can be shown that $\{\sigma_i^+\sigma_j^-\}$ (allowing $i = j$) generates SA n, and $\{\sigma_i^+\sigma_j^-, \sigma_i^-\sigma_j^-, \sigma_i^+\sigma_j^+\}$ generate SAp [17].

Hamiltonians and universal sets without single-qubit operations.— Now consider the properties of Hamiltonians relevant to scalable proposals for quantum computing. A generic time-dependent Hamiltonian [1–7,9] has the form

$$\begin{aligned} H(t) &\equiv H_0 + V + F \\ &= \sum_i \frac{1}{2}\varepsilon_i(t)\sigma_i^z + \sum_{i<j}\sum_{\alpha,\beta=x,y,z} J^{\alpha\beta}_{ij}(t)\sigma_i^\alpha\sigma_j^\beta \\ &\quad + \sum_i \left(f_i^x(t)\sigma_i^x + f_i^y(t)\sigma_i^y\right). \end{aligned} \quad (4)$$

The first term is the sum of single-qubit energies, (with $\varepsilon_i/\hbar$ being the frequency of the $|0\rangle_i \to |1\rangle_i$ transition) and is often controllable using local potentials. The second term is the two-qubit interaction, which we assume can be turned on/off at controllable times t. The third term is the (potentially problematic) external field, often pulsed, used to manipulate single qubits. By turning the controllable parameters on/off one has access to a set of Hamiltonians $\{H_i\}$, which can be used to generate unitary logic gates through the following three processes: (i) *Arbitrary phases* are obtained by switching an H_i on for a fixed time. (ii) *Adding* or (iii) *commuting Hamiltonians* can be approximated by using a finite number of terms in the Lie sum and product formulas, e.g. [9,10], $e^{i(\alpha A+\beta B)} = \lim_{n\to\infty}\left(e^{i\alpha A/n}e^{i\beta B/n}\right)^n$, implying that the Hamiltonians A, B are switched on/off alternately. These operations are experimentally implementable and suffice to cover the Lie group generated by the set $\{H_i\}$. In practice it may be easier to use Euler angle rotations rather than infinitesimal steps [16], as done routinely in NMR [9]. Let us now specialize to the case $J^{\alpha\beta}_{ij} = J^\alpha_{ij}\delta_{\alpha\beta}$ (denoting V by V') which amounts to limiting the Hamiltonian to exchange-type interactions, that appear to be most relevant for solid-state QC. Using $\sigma_i^\pm, n_i$ we find

$$H_0 = \sum_i \varepsilon_i\left(\frac{1}{2} - n_i\right), \quad F = \sum_i \left(f_i^*\sigma_i^- + f_i\sigma_i^+\right), \quad (5)$$

$$V' = \sum_{i<j}\left(\Delta_{ij}(\sigma_i^-\sigma_j^- + \sigma_i^+\sigma_j^+) + J_{ij}(\sigma_i^+\sigma_j^- + \sigma_j^+\sigma_i^-)\right. \quad (6)$$
$$\left. + J^z_{ij}\sigma_i^z\sigma_i^z\right) \quad (7)$$

where

$$f_i = (f_i^x - if_i^y), \quad \Delta_{ij} = J^x_{ij} - J^y_{ij}, \quad J_{ij} = J^x_{ij} + J^y_{ij}.$$

The above analysis of the subalgebras of $U(2^N)$ now helps us in drawing certain general conclusions. (i) By appending σ_i^-, σ_i^+ to the set generating SAp it becomes possible to transform between states differing by an odd occupation number. Thus the set $\{\sigma_i^+\sigma_j^-, \sigma_i^-\sigma_j^-, \sigma_i^+\sigma_j^+, \sigma_i^-, \sigma_i^+\}$ suffices to generate $SU(2^N)$. This establishes the well-known universality of H. (ii) When $F = 0$, $[H_0 + V', \widehat{p}] = 0$, so $H_0 + V'$ is in SAp. This implies that this Hamiltonian by itself is *not fully universal*: it operates on a 2^{N-1}-dimensional invariant subspace. (iii) Recalling that single qubit operations are often difficult, which two-qubit interactions are sufficient for universality? Ref. [10] established that two-body Hamiltonians are "generically" universal. The genericness condition was stated in terms of abstract group-theoretic properties. Here we are able to state the condition more explicitly for the class of Eq. (4). Define the parity of an operator according to whether the total number of raising and lowering operators is even or odd (e.g., n_1 is even, but $\sigma_2^- n_1$ is odd.). The necessary condition for a Hamiltonian to be universal is that it contains an odd term, so that the system can leave SAp. If $F = 0$ there does not exist an odd term in $H(t)$. Hence the next step is to reconsider the most general interaction with $J^{\alpha\beta}_{ij}$ arbitrary. H of Eq. (4) is universal for $F = 0$ if and only if there exists one of the odd terms $\sigma_i^z\sigma_j^x = (1 - 2n_i)(\sigma_j^+ + \sigma_j^-)$ or

$\sigma_i^z\sigma_j^y$. Such terms may arise due to perturbative spin-orbit coupling corrections to the isotropic part $J_{ij}(t)\overrightarrow{\sigma}_i\cdot\overrightarrow{\sigma}_j$ [where $\overrightarrow{\sigma}_i=(\sigma_i^x,\sigma_i^y,\sigma_i^z)$] of Eq. (4). E.g., a recent estimate of the coupling strength of the antisymmetric (Dzyaloshinskii-Moriya) spin exchange term $\overrightarrow{d_{ij}}\cdot(\overrightarrow{\sigma}_i\times\overrightarrow{\sigma}_j)$ shows $|\overrightarrow{d_{ij}}|/J_{ij}$ to be as large as 0.01 for coupled quantum dot in GaAs [18]. Unlike the isotropic exchange parameter $J_{ij}(t)$, $\overrightarrow{d_{ij}}$ is typically *not* controllable. Nevertheless, its very presence allows for universal QC without the external field F. To see this, suppose for simplicity that $\overrightarrow{d_{ij}}$ is along the x-axis [so that $\overrightarrow{d_{ij}}\cdot(\overrightarrow{\sigma}_i\times\overrightarrow{\sigma}_j)=d_{ij}(\sigma_i^y\sigma_j^z-\sigma_i^z\sigma_j^y)$], and that the terms $\overrightarrow{\sigma}_i\cdot\overrightarrow{\sigma}_j$, σ_i^z are controllable while $\sigma_i^y\sigma_j^z-\sigma_i^z\sigma_j^y$ is small and not controllable. Then we can show that these operators generate the group $SU(4)$ on the qubit pair i,j and therefore are universal. The Hamiltonian is $H_{ij}=d_{ij}(\sigma_i^y\sigma_j^z-\sigma_i^z\sigma_j^y)+\frac{1}{2}(\varepsilon_i\sigma_i^z+\varepsilon_j\sigma_j^z)+J_{ij}\overrightarrow{\sigma}_i\cdot\overrightarrow{\sigma}_j$. When turning off the parameters $\varepsilon_i,\varepsilon_j$ and J_{ij}, one gets the gate generated by the antisymmetric term $\sigma_i^y\sigma_j^z-\sigma_i^z\sigma_j^y$ by just waiting. Since this term is very small compared to J_{ij}, to a good approximation we can neglect its effect when we turn on other terms, e.g., $H_{ij}\approx J_{ij}(t)\overrightarrow{\sigma}_i\cdot\overrightarrow{\sigma}_j$ when turning on J_{ij}. We can then show that $SU(4)$ can be generated by commutation. E.g., $\sigma_i^y=[[\sigma_i^y\sigma_j^z-\sigma_i^z\sigma_j^y,\overrightarrow{\sigma}_i\cdot\overrightarrow{\sigma}_j],\sigma_i^z]/2$, and similarly, we can generate σ_j^y. Therefore, we have the gate set generated by $\{\sigma_i^y,\sigma_j^y,\sigma_i^z,\sigma_j^z,\overrightarrow{\sigma}_i\cdot\overrightarrow{\sigma}_j\}$ which is known to be universal. It is interesting to note that the approximation assuming a small antisymmetric term is not necessary [17]. If control over ε_i is unavailable one may have to resort to other methods [17,20].

Elimination of single-qubit operations through encoding.— Our discussion of universality so far assumed that one is seeking to employ the full 2^N-dimensional Hilbert space of N qubits. However, it was apparent from this discussion that the symmetries of a given Hamiltonian determine an invariant subspace and that in physically generic circumstances this subspace has reduced dimensionality. A common solution is to introduce an external field which breaks the symmetry. As discussed above this often leads to significant engineering complications . However, as shown first in [13] for the case of isotropic exchange, a Hamiltonian may still be *computationally universal over a subspace*, for the price of using several physical qubits to encode a logical qubit. Here we analyze this concept for the anisotropic members of the class of Hamiltonians H_0+V'. In each case we assume that no external single qubit operations are used, i.e., $F=0$, and give an encoded universal set of gates. As distinct from [12–16] we explicitly take H_0 into account, as this is a term that is generally difficult to turn off. Our analysis provides simple encoding procedures along with explicit recipes for universal computation in situations of experimental interest.

Axial Symmetry.— Assume $\Delta_{ij}=0$. This axial symmetry is the case, e.g., for the electrons floating on helium proposal [7]. The major handle there is the single-qubit energies ε_i, which allows to tune the qubits into and out of resonance with externally applied radiation. This tuning is used to control the parameters f_i, J_{ij}^z and J_{ij} of Eqs. (5),(6). However, it is advantageous to do away with controlling the single qubit parameters f_i, as they are manipulated via a global and slow microwave field. Limitations related to other QC proposals were discussed above. Motivated by these difficulties a solution involving control of only the $\sigma_i^x\sigma_j^x+\sigma_i^y\sigma_j^y$ term was proposed in [12], encoding a qutrit into three physical qubits. Here we give a more economical solution: we show how to compute universally on a logical qubit encoded into only two physical qubits. Our solution makes use of the naturally available H_0 term, and assumes that the J_{ij}^z and J_{ij} parameters can be tuned separately. In fact not all of these parameters need to be independently controllable, as discussed below. Since in the axial symmetry case V' preserves occupation number, the encoding is simply $|0_L\rangle_m=|0\rangle_{2m-1}|1\rangle_{2m}$ and $|1_L\rangle_m=|1\rangle_{2m-1}|0\rangle_{2m}$ for the m^{th} logical qubit. To implement single-encoded-qubit operations assume we can selectively turn on nearest-neighbor interactions $J_{2m-1,2m}$ and $J_{2m-1,2m}^z$ in pairs encoding a qubit (i.e., $J_{2m,2m+1}=J_{2m,2m+1}^z=0$). Using the definitions (2),(3) with $\mu\equiv m$ when $i=2m-1$ and $j=2m$, we can rewrite the Hamiltonian (4) as:

$$H_{\text{AS}}=\sum_{m=1}^{N/2}\left(\frac{\epsilon_m}{2}T_m^z+J_mT_m^x\right)+h_1+h_0, \tag{8}$$

where $\epsilon_m\equiv\varepsilon_{2m-1}-\varepsilon_{2m}$, $J_m\equiv J_{2m-1,2m}$, $\omega_m=\varepsilon_{2m-1}+\varepsilon_{2m}$, $h_1\equiv\sum_{m=1}^{N/2}\frac{1}{2}\omega_mR_m^z$, and $h_0\equiv\sum_{m=1}^{N/2}J_{2m-1,2m}^z\left((R_m^z)^2-(T_m^z)^2\right)$. The term h_0 is an energy shift which commutes with all other operators, and will thus be neglected. It is then clear that H_{AS} is a sum over independent modes m, so that the Hilbert space decomposes into a tensor-product structure. The operators T_m^z,T_m^x generate an encoded $SU_m^t(2)$ group, while the term $h_1\in su_m^r(2)$ acts as a constant (since $[su_m^t(2),su_m^r(2)]=0$). As a whole H_{AS} acts as $\bigotimes_{m=1}^{N/2}SU_m^t(2)$, meaning that experimental control over the coefficients ϵ_m and J_m enables the implementation of independent and arbitrary encoded-single qubit operations. Next we need to show how to implement an encoded controlled operation. This can be done very simply using nearest-neighbor interactions only. All that is required is to turn on the coupling $J_{2m,2m+1}^z$, since as is easily checked $\sigma_{2m}^z\sigma_{2m+1}^z=-T_m^zT_{m+1}^z$. This yields a controlled-phase gate [9]. It may appear from this discussion that all ϵ_m, J_m and $J_{2m,2m+1}^z$ should be controllable. However, in analogy to NMR, we can further show that *independent control over the coefficients* J_m *suffices to generate arbitrary single-encoded qubit operations and an encoded controlled operation.* Suppose that ϵ_m and $J_{2m,2m+1}^z$ are not directly controllable, as is the

case for the analogous parameters in front of the terms σ_i^z and $\sigma_i^z \sigma_j^z$ in a typical liquid-state NMR Hamiltonian. *Refocusing* in terms of T_m^x then plays the same role as refocusing using σ^x in NMR [9], allowing control over ϵ_m and $J_{2m,2m+1}^z$. This "encoded refocusing" method will be treated in detail in a separate publication [17].

Decoherence Avoidance.— The connection between encoding and immunity to decoherence is known from the theory of decoherence-free subspaces (DFSs) [21]. The present encoding is decoherence-free under the following conditions: Assume that the system-bath interaction is $H_I = \sum_{i=1}^N \sigma_i^z \otimes B_i^z$ where B_i^z are bath operators. If pairs of qubits are sufficiently close compared to the bath wavelength, so that $B_{2m-1}^z = B_{2m}^z \equiv \tilde{B}_m^z$ ("block-collective phase damping" [21]) then $H_I \to H_I^{\rm CPD} = 2\sum_{m=1}^{N/2} R_m^z \otimes \tilde{B}_m^z$. But $R_m^z \left(\alpha|0_L\rangle_m + \beta|1_L\rangle_m\right) = 0$ so that the interaction $H_I^{\rm CPD}$ does not cause decoherence. Furthermore, $H_I^{\rm CPD}$ commutes with $H_{\rm AS}$ and with $T_m^z T_{m+1}^z$, so it follows from a general theorem [13,22] that with the methods provided above universal encoded logic can be implemented without ever leaving the DFS.

Axially Asymmetric Interaction.— Assume that one can control the axial asymmetry parameter $\Delta_{ij} = J_{ij}^x - J_{ij}^y$ in Eq. (6). Further assume only nearest-neigbor interactions in pairs are on, and let $\Delta_m \equiv \Delta_{2m-1,2m}$. The Hamiltonian $H_0 + V'$ now becomes:

$$H_{\rm AA} = \sum_{m=1}^{N/2} \left(\frac{\epsilon_m}{2} T_m^z + J_m T_m^x\right) + \left(\frac{\omega_m}{2} R_m^z + \Delta_m R_m^x\right),$$

where we have again omitted the h_0 term. The appropriate encoding for the $R_m^{z,x}$ terms is: $|0_L\rangle_m = |0\rangle_{2m-1}|0\rangle_{2m}$, $|1_L\rangle_m = |1\rangle_{2m-1}|1\rangle_{2m}$ for the $m^{\rm th}$ logical qubit, since the axially asymmetric component of the Hamiltonian preserves parity but not occupation number. To implement a controlled operation on the $m^{\rm th} \otimes m+1^{\rm th}$ encoded-qubits' Hilbert space it suffices again to turn on the nearest neighbor coupling $\Delta_{2m,2m+1}$, since $\sigma_{2m}^z \sigma_{2m+1}^z = R_m^z R_{m+1}^z$. In analogy to the analysis above, the subspace acted on by $su_m^t(2)$ operators is furthermore decoherence-free if the system-bath interaction $H_I = \sum_{i=1}^N \sigma_i^z \otimes B_i^z$ has the symmetry $B_{2m-1}^z = -B_{2m}^z$. The two subspaces acted upon by the axially symmetric and antisymmetric terms are independent. They can be regarded as two independent quantum computers.

State Preparation and Measurement.— The state $\left(|01\rangle - |10\rangle\right)/\sqrt{2} = \left(|0_L\rangle - |1_L\rangle\right)/\sqrt{2}$ is the ground state of the axially symmetric Hamiltonian $\sigma^x\sigma^x + \sigma^y\sigma^y$, while $\left(|00\rangle - |11\rangle\right)/\sqrt{2} = \left(|0_L\rangle - |1_L\rangle\right)/\sqrt{2}$ is the ground state of the axially antisymmetric Hamiltonian $\sigma^x\sigma^x - \sigma^y\sigma^y$. Thus by lowering the temperature to below J and Δ (the respective strengths of the interactions), the system will relax into the corresponding subspaces and computation can begin. Measurement can be done in the axially symmetric case by first applying an encoded Hadamard gate [which maps $|0_L\rangle \to \left(|0_L\rangle + |1_L\rangle\right)/\sqrt{2}$, $|1_L\rangle \to \left(|0_L\rangle - |1_L\rangle\right)/\sqrt{2}$], and then using, e.g., Kane's a.c. capacitance scheme [2], which distinguishes a singlet from a triplet state. In the axially antisymmetric case Kane's scheme will distinguish the states $\left(|00\rangle \pm |11\rangle\right)/\sqrt{2}$, so the same procedure applies.

Conclusions.— We studied here the quantum computational power of a generic class of anisotropic solid-state Hamiltonians. We presented simple encodings of one qubit into two physical qubits, and schemes which enable universal computation in the case of axially symmetric and/or antisymmetric exchange-type Hamiltonians, while avoiding difficult-to-implement single-qubit control terms. Only nearest-neighbor interactions are needed for this implementation of encoded universal quantum logic. These results can be generalized to provide codes with higher rates [17]. The methods presented here have the potential to offer significant simplifications in the construction of QCs based on quantum dots, donor-atom nuclear or electron spins, quantum Hall systems, and electrons floating on helium.

Acknowledgements.— We thank A. Blais and A. Maassen v.d. Brink for helpful discussions. DAL gratefully acknowledges financial support from PREA, NSERC, and the Connaught Fund.

[1] D. Loss and D.P. DiVincenzo, Phys. Rev. A **57**, 120 (1998).
[2] B.E. Kane, Nature **393**, 133 (1998).
[3] R. Vrijen *et al.*, Phys. Rev. A **62**, 012306 (2000).
[4] V. Privman *et al.*, Phys. Lett. A, **239**, 141 (1998).
[5] A. Imamoglu *et al.*, Phys. Rev. Lett. **83**, 4204 (1999).
[6] S.-B. Zheng and G.-C. Guo, Phys. Rev. Lett. **85**, 2392 (2000).
[7] P.M. Platzman and M.I. Dykman, Science **284**, 1967 (1999).
[8] A. Barenco *et al.*, Phys. Rev. A **52**, 3457 (1995);
[9] M.A. Nielsen and I.L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, UK, 2000).
[10] S. Lloyd, Phys. Rev. Lett. **75**, 346 (1995).
[11] D. Gottesman, Phys. Rev. A **57**, 127 (1997).
[12] D. Bacon *et al.*, eprint quant-ph/0102140.
[13] D. Bacon *et al.*, Phys. Rev. Lett. **85**, 1758 (2000).
[14] P. Zanardi, Phys. Rev. A **63**, 012301 (2001); D.A. Lidar *et al.*, Phys. Rev. A **63**, 022307 (2001); L. Viola *et al.*, eprint quant-ph/0101090;
[15] J. Kempe *et al.*, Phys. Rev. A **63**, 042307 (2001).
[16] D.P. DiVincenzo *et al.*, Nature **408**, 339 (2000).
[17] L.-A. Wu and D.A. Lidar, in preparation.
[18] K.V. Kavokin, eprint cond-mat/0011340.
[19] We use the convention that upper-case (lower-case) denotes a Lie group (algebra).
[20] N.E. Bonesteel *et al.*, eprint quant-ph/0106161.

[21] P. Zanardi and M. Rasetti, Phys. Rev. Lett. **79**, 3306 (1997); L.-M Duan and G.-C. Guo, Phys. Rev. A **57**, 737 (1998); D.A. Lidar *et al.*, Phys. Rev. Lett. **81**, 2594 (1998).

[22] P. Zanardi, Phys. Rev. A **60**, R729 (2000); E. Knill *et al.*, Phys. Rev. Lett. **84**, 2525 (2000)